UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,786	09/05/2006	Sebastien Canard	33901-220PUS	4281

7590 06/10/2009

Thomas Langer
Cohen Pontani Lieberman & Pavane
Suite 1210
551 fifth Avenue
New York, NY 10176

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
06/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/591,786	CANARD ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/3/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to Amendment filed 3/3/3009. Claims 1-18 are amended. Claims 19-21 are new. Claims 1-21 are pending.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Applicant's recites in claims 12, 14, 16, and 18 a "computer readable medium". The Examiner contends applicant's specification does not provide proper antecedent basis for such a claim limitation element.

Claim Objections

2. Claims 4 and 7 are objected to because of the following informalities: The Examiner position is that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim. The Examiner contends claims 4 and 7 depend on claim 20 and are therefore improper dependent claims. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 6 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The Examiner contends applicant's newly amended claim subject matter of, "if a particular mix-server (M_i) of said second mix-net (M) does not generate a satisfactory zero knowledge proof of the knowledge as a result of said prompting step" lacks support of original disclosure.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-21 rejected under 35 U.S.C. 103(a) as being unpatentable over Fujioka et al. (US Patent No. 6,845,447 and Fujioka hereinafter) in view of Chaum (European Patent No. 0139313 B1 (cited from IDS)).

5. As to claim 1, Fujioka teaches a electronic voting method comprising the steps of obtaining from a signer apparatus using a fair blind signature scheme, a digital signature (Yi) of a data signal (xi) from a voter apparatus, said data signal comprising a vote (I~i)) of a voter and (i.e., ... teaches A voter V.sub.i encrypts his vote content v.sub.i with a public key k.sub.PC of a counter C, then concatenates the encrypted vote content x.sub.i with a tag t.sub.i to obtain a ballot z.sub.i, then randomizes it with a random number r.sub.i to create a preprocessed text

e.sub.i, and sends it and a signature s.sub.i therefor to an election administrator A .... teaches a administrator A generates a blind signature d.sub.i for the preprocessed text e.sub.i and sends it back to the voter V.sub.i .... teaches a voter V.sub.i excludes the influence of the random number r.sub.i from the blind signature d.sub.i to obtain administrator signature y.sub.i, and sends vote data to a counter C.[abstract].

Fujoka does not expressly teach:

establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated,

said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25]), said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme (to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

6. As to claim 2, Fujioka teaches a electronic voting where the fair blind signature scheme is comprises a threshold fair blind signature scheme in which the digital

signature is obtained from a sub-set of a group of servers which form said signer apparatus, the group of servers containing n servers and the sub-set containing t servers, where t < n (i.e., ... teaches the decryption process involves the use of a distributed secret key k.sub.SCj of every distributed counter, or requires a certain number (a threshold value U.sub.t [abstract])

7. As to claim 3, Fujioka teaches a electronic voting method where the data signal (xi) corresponds to the vote (v_i) of the voter which is encrypted according to a first encryption scheme (ErM) (i.e., ... teaches A voter V.sub.i encrypts his vote content v.sub.i with a public key k.sub.PC [abstract]),

said first encryption scheme being the encryption scheme of a first mix-net (TM) contained in a voter-tallying module [300, fig 1], and the method further comprises the step of using said first mix-net (T<) to apply a decryption scheme (D_{TM}) which is an inverse of said first encryption scheme to said data signal (xi) at said voter tallying module to retrieve the vote (v_i) of the voter (i.e., … teaches a voter tally module [300, fig. 1] …further teaches a decryption scheme applied [fig. 5]).

8. As to claim 4, Fujioka teaches a voting method and comprising the steps of:

receiving, by a ballot-order-randomizing module [130, fig. 3] , a batch of encrypted data signals (c_i) (e.g., encrypted vote content) from said ballot-box module [abstract], said encrypted data signals (e.g., encrypted vote content) being in a first order within said batch of encrypted data signals (c_i) [abstract], each encrypted data

signal (c_i) (e.g., encrypted vote content) comprising data encrypted according to a second encryption scheme (E_M) and said data including a respective data signal (x_i) the encrypted data signal (c_i) including the vote (v_i) of the voteer subjected to plural levels of encryption (i.e., ... teachers encrypting vote content with public key. The vote content containing voter's vote [abstract]);

retrieving, in said ballot-order-randomizing module, each respective data signal (x_i) from the respective encrypted data signal (c_i) in said batch of encrypted data signals (c_i) by applying a decryption scheme (D_M) which is an inverse said second encryption scheme (E_M) (i.e., ... teaches the encrypted vote are decrypted [col. 3, lines 10-20]);

and outputting the retrieved data signals (x_i) for said batch of encrypted data signals (c_i) in a different order from said first order [fig. 3]:

and receiving, by said vote-tallying module [300, fig. 1}, said retrieved data signals (x_i) said different order [S1, fig. 1].

9. As to claim 5, Fujioka teaches a electronic voting method where said second encryption scheme is the encryption scheme of a second mix-net (M) [abstract], in said ballot-order-randomizing module (130, fig. 3), said second mix-net comprising a plurality of mix-servers (e.g., counter apparatus] [300, fig. 1].

10. As to claim 6, Fujioka teaches a voting method comprising the step of:

detecting irregularities in one or more ballots to be counted do not contain duplicated data-pairs (i.e., ... teaches and makes a check in the list checking part 170 to

see if the number of ballots placed on the ballot list 320A is equal to the number of voters published [col. 8, lines 20-30]), wherein a data-pair corresponds to one of said data signals and the digital signature thereof [fig. 6], for each of said one or more ballots {fig. 2C], said mix-servers of said second mix-net (M) (e.g., counter) being prompted to generate zero-knowledge proofs of knowledge (i.e., ... teaches a anonymous (e.g., zero knowledge) communication [col. 9, lines 45-50]);

and if a particular mix-server (M_i) of said second mix-net (M) does not generate a satisfactory zero knowledge (e.g., anonymous) proof of the knowledge as a result of said prompting step (col. 9, lines 60-65), applying said decryption scheme (D_M) which is the inverse of said second encryption scheme (E_M) using said second mix-net (M) which excludes said particular mix-server (M_i) to retrieve said data signals (x_i) (i.e., ... teaches a decryption scheme applied to decrypted encrypted vote content [col. 2, lines 50-60]).

11. As to claim 7, Fujioka teaches a voting method further comprising the step of detecting irregularities in the voting process, wherein the step of comparing vote data held by the signer apparatus with vote data held by the ballot box module (S5, fig. 6), to detect irregularities comprises checking the validity of the digital signatures in the one or more ballots to be counted (i.e., .. teaches checking the verification of the digital signatures compliance to equation [col. 8, lines 1-10]).

12. As to claim 8, Fujioka teaches a voting method further comprising the step of:

and including said identified signed data signals in a revocation list (e.g., authorized voter list) recording ballots that have been rejected (i.e., ...teaches verifying vote content (e.g. signed data signal) for purpose of invalidity [col. 8, lines 30-40] ... further teaches a list containing voter [col. 6, lines 58-61]).

Fujoka does not expressly teach:

controlling said trusted authority apparatus such that said tracing protocol of said fair blind signature scheme is applied to identify the signed data signals corresponding to said one or more ballots to be counted (to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)];

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

controlling said trusted authority apparatus such that said tracing protocol of said fair blind signature scheme is applied to identify the signed data signals corresponding to said one or more ballots to be counted (to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)];

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items

and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

13. As to claim 9, Fujioka teaches a voting method of claim 1 and further comprising the steps of:

receiving said data signal (x_i) for digital signature according to said fair blind signature scheme at a server module of said signer apparatus, said data signal (xi) comprising a vote (vi) selected by a voter (VI), said vote (vi) being encrypted according to a first encryption scheme (ETM), blinded according to said fair blind signature scheme and digitally signed according to a digital signature scheme of said voter [abstract];

verifying, by said server module, that the digital signature (si) in the received signal is valid (i.e., .. teaches checking the verification of the digital signatures compliance to equation [col. 8, lines 1-10]);

in caese where the verifying step confirms that the digital signature in the signal received by said server module is valid, said server module digitally signs the blinded encrypted vote (e_i) according to said fair blind digital scheme and outputs the digitally-signed message (SAs(ei)) [abstract];

unblinding the digitally-signed message (SAs(ei)) to yield said digital signature (3/) of the data signal (xi) [abstract];

encrypting said data signal (xi) and said digital signature (Y_i) of the data signal thereof according to a second encryption scheme (E_M) to produce encrypted data signal

(c_i) (i.e., ... teaches each voter encrypts his vote content by a public key of the counter, then randomizes the encrypted vote content by a random number to create a preprocessed text, then attaches thereto his signature, and sends the signed text to the election administrator [col. 2, lines 33-40]);

and signing said encrypted data signal according to the digital signature scheme of the voter (V_i) [abstract].

14. As to claim 10, Fujioka teaches a electronic voting system comprising:

a plurality of voter modules each including a first processor (100, fig. 1);

and an admin server module including a second processor (200, fig. 1);

wherein the first processor, a voter module and the second processor in the admin server module cooperate in during a respective signing session in application of a fair blind signature scheme to obtain (i.e., … teaches admin module utilizes a blind signature scheme [abstract]), from said admin server module a digital signature (Y_i) of a data signal (x_i) from a voter module [abstract], said data signal (x_i) (e.g., vote content) comprising a respective vote (v_i) of a voter [abstract[),

Fujioka does not expressly teach:

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

said fair blind signature scheme (e.g., blind signature scheme) having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25] and further to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

15. As to claim 11, Fujioka teaches a voter module including a first processor configured to cooperate with a second processor in an admin server module during a respective signing session in application of a fair blind signature scheme to obtain [abstract}, from said admin server module [fig. 1], a digital signature (Y_i) of a data signal

(x_i) from the voter module [abstract], said data signal (x_i) comprising a vote (v_i) of a voter [abstract],

Fujioka does not expressly teach:

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

said fair blind signature scheme (e.g., blind signature scheme) having a tracing protocol (e.g., correspondence determination means) which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25] and further to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items

and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

16. As to claim 12, Fujioka teaches a computer-readable medium encoded with a computer program executed by a computer that causes a first processor to cooperate with a second processor in an admin server module during a respective signing session in application of a fair blind signature scheme [fig. 1; abstract], the computer program comprising:

program code for obtaining, from said admin server module [200, fig 1], a digital signature (y_i) of a data signal (x_i), said data signal (x_i) comprising a vote (v_i) of a voter [abstract];

Fujoka does not expressly teach:

establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25]), said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme (to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

17. As to claim 13, Fujioka teaches a voting system admin server module (20) adapted to cooperate with a voter module (10) in application of a fair blind signature scheme whereby to obtain a digital signature 0'i) of a data signal (xi) comprising the voter's vote (vl) (i.e., ... teaches A voter V.sub.i encrypts his vote content v.sub.i with a public key k.sub.PC of a counter C, then concatenates the encrypted vote content x.sub.i with a tag t.sub.i to obtain a ballot z.sub.i, then randomizes it with a random number r.sub.i to create a preprocessed text e.sub.i, and sends it and a signature s.sub.i therefor to an election administrator A .... teaches a administrator A generates a

blind signature d.sub.i for the preprocessed text e.sub.i and sends it back to the voter V.sub.i .... teaches a voter V.sub.i excludes the influence of the random number r.sub.i from the blind signature d.sub.i to obtain administrator signature y.sub.i, and sends vote data to a counter C.[abstract]).

18. As to claim 13, Fujioka teaches a voting system admin server module including a first processor configured to cooperate with a second processor in a voter module during a respective signing session in application of a fair blind signature scheme to obtain [fig. 1], from said admin server module (200, fig. 1), a digital signature (Y_i) of a data signal (X_i) from said voter module, said data signal (X_i) comprising a vote (v_i) of a voter [abstract],

Fujoka does not expressly teach:

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to link a given digitally-signed data signal with a signing session in which said digital signature was generated by said admin server module.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

said fair blind signature scheme (e.g., blind signature scheme) having a tracing protocol (e.g., correspondence determination means) which enables a trusted authority

apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25] and further to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

19. As to claim 14, Fujioka teaches a computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system admin server module (20) according to claim 13 (i.e., ... teaches election administrator verifies the validity of the voter through utilization of his signature attached to the encrypted text [col. 2, lines 35- 40].

20. As to claim 14, Fujioka teaches a computer-readable medium encoded with a computer program that causes a first processor to cooperate with a second processor in a voter module during a respective signing session in application of a fair blind signature scheme [abstract], the computer program comprising: program code for obtaining a

digital signature (y_i) of a data signal (X_i) from said voter module, said data signal (X_i) comprising a vote (v_i) of a voter [abstract];

Fujoka does not expressly teach:

and program code for establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

and program code for establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25]), said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme (to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying

Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

21. As to claim 15, Fujioka teaches a voting system ballot-order randomizer module comprising: a processor configured to provide input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (c_i) comprising data (x_i) indicative of a respective vote (v_i) digitally signed according to a fair blind signature scheme [abstract], , each encrypted data signal (c_i) being encrypted according to a predetermined encryption scheme (E_M) (i.e., ... teaches each voter encrypts his vote content by a public key of the counter, then randomizes the encrypted vote content by a random number to create a preprocessed text, then attaches thereto his signature, and sends the signed text to the election administrator [col. 2, lines 33-40]);

and a mix-net (M) for decrypting said encrypted data signals (c_i) (e.g., encrypted vote content) by applying a decryption scheme (D_M) which is an inverse to said predetermined encryption scheme (EM) (i.e., ... teaches a decryption scheme applied to decrypted encrypted vote content [col. 2, lines 50-60]);

and output means for outputting the decrypted signals of said batch of cast votes in an order different from the order of the corresponding encrypted data signals in said batch of cast votes [fig. 3].

Fujioka does not expressly teach:

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally signed data signal and a signing session in which said digital signature was generated,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

said fair blind signature scheme (e.g., blind signature scheme) having a tracing protocol (e.g., correspondence determination means) which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25] and further to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

22. As to claim 16, Fujioka teaches a computer-readable medium encoded with a computer program that causes a voting system ballot-order-randomizer to randomize a batch of cast votes [130, fig. 3], the computer program comprising:

program code for receiving, at an input means (400, fig. 1), a batch of cast votes (S4, fig. 6), each cast vote comprising an encrypted data signal (c_i) comprising data indicative of a respective vote (v_i) of a voter which is digitally signed according to a fair blind signature scheme [abstract], each encrypted data signal (e) (e.g., voter content) being encrypted according to a predetermined encryption scheme (E_M) program code for decrypting (i.e., ...teaches decrypting process [abstract])), at a mix-net (M), said encrypted data signals (c_i) (e.g., encrypted vote content) by applying a decryption scheme (D_M) which is an inverse of said predetermined encryption scheme (E_M) (i.e., ... teaches a decryption scheme applied to decrypted encrypted vote content [col. 2, lines 50-60]);

and program code for outputting, at an output means (fig. 8B), the decrypted signals of said batch of cast votes in an order different from the order of corresponding encrypted data signals in said batch of cast votes (S6, fig. 6).

Fujioka does not expressly teach:

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

said fair blind signature scheme (e.g., blind signature scheme) having a tracing protocol (e.g., correspondence determination means) which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25] and further to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

23. As to claim 17, Fujioka teaches a voting system tallier module (50) comprising: input means for receiving cast votes [fig. 7], each cast vote comprising a data signal (x~) digitally signed according to a fair blind signature scheme (i.e., ... teaches a blind signature [abstract]), each data signal (xi) comprising a respective voter's vote (vi)

encrypted according to an encryption scheme (EM) (i.e., ... teaches encrypted vote content [abstract]);

and a mix-net (M) for decrypting said encrypted votes (vi) (e.g., encrypted vote content) by applying a decryption scheme (DM) inverse to said encryption scheme (EM) (i.e., ... teaches a decryption scheme applied to decrypted encrypted vote content [col. 2, lines 50-60]).

24. As to claim 17, Fujioka teaches a voting system module comprising a processor configured to provide: input means for receiving cast votes, each cast vote comprising a data signal (x_i) digitally signed according to a fair blind signature scheme, each data signal (x_i) comprising a respective vote (vi) of a voter which is encrypted according to an encryption scheme (E_M) [abstract];

and a mix-net (M) for decrypting said encrypted votes (v_i) (e.g., encrypted vote content) by applying a decryption scheme (D_M) which is an inverse of said encryption scheme (E_M) (i.e., ... teaches a decryption scheme applied to decrypted encrypted vote content [col. 2, lines 50-60]).

Fujioka does not expressly teach:

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

said fair blind signature scheme (e.g., blind signature scheme) having a tracing protocol (e.g., correspondence determination means) which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25] and further to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

25. As to claim 18, Fujioka teaches a computer-readable medium encoded with a computer program that causes tallying of cast votes [300, fig. 1], the computer program comprising: program code for receiving, at an input means, cast votes, each cast vote comprising a data signal (x_i) (e.g., vote content) digitally signed according to a fair blind signature scheme [abstract], each data signal (x_i) comprising a respective vote (v_i) of a

voter which is encrypted according to an encryption scheme program code for decrypting [abstract],

-at a mix-net (M), said encrypted votes (v_i) (e.g., encrypted vote content) by applying a decryption scheme (D_M) which is an inverse of said encryption scheme (E_M) (i.e., ... teaches a decryption scheme applied to decrypted encrypted vote content [col. 2, lines 50-60]),

Fujioka does not expressly teach:

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

said fair blind signature scheme (e.g., blind signature scheme) having a tracing protocol (e.g., correspondence determination means) which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated (to provide the link establishing capability between things having a signature property and items received for signing (e.g., signing session) [pg. 7, lines 15-25] and further to provide means to determine correspondence (e.g., tracing protocol) [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of establishing links between signed items and received items for signing as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

26. As to claim 19, Fujoka teaches a voting method where the data signal (xi) corresponds to the vote (v_i) of the voter which is encrypted according to a first encryption scheme (E_M) (abstract), said first encryption scheme comprising an encryption scheme of a vote-tallying module [300, fig. 1], and the method further comprising the step of applying a decryption scheme (D_M) which is an inverse of said first encryption scheme to said data signal (Xi) at said vote-tallying module to retrieve the vote (vi) of the voter (i.e., ... teaches a applying a decryption scheme [abstract].

27. As to claim 20, Fujoka teaches a voting method further comprising the steps of setting a time period during which voting is authorized (i.e., ... teaches predetermined time period availibility [col. 7, lines 40-50]);

communicating a plurality of encrypted data signals (ci) to a ballot-box module, each of said plural encrypted data signals (ci) (e.g., encrypted voter content) including data from a respective voter indicative of the vote (vj) of said voter and digitally-signed by said signer apparatus [abstract]; and outputting, by said ballot-box module [320, fig.

1], said encrypted data signals (ci) (e.g., encrypted voter content [abstract]) to said vote-tallying module after expiration of the time period in which voting is authorized (i.e., ...teaches a time period expiration [col. 7, lines 40-50].

28. As to claim 21, Fujoka teaches a voting further comprising the steps of: and including said identified signed data signals (e.g., voter content) in a revocation list recording ballots that have been rejected (i.e., ... teaches maintaining a list for the purpose of authorizing ballots [240, fig. 1].

Fujoka does not expressly teach:

controlling said trusted authority apparatus such that said tracing protocol of said fair blind signature scheme is applied to identify signed data signals corresponding to said one or more of the ballots to be counted;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Fujoka as introduced by Chaum. Chaum discloses:

controlling said trusted authority apparatus such that said tracing protocol (e.g., correspondence determination means) of said fair blind signature scheme (e.g., blind signature scheme) is applied to identify signed data signals corresponding to said one or more of the ballots to be counted (to provide means to determine correspondence (e.g., tracing protocol) of blind signature scheme [(pg.7, lines 25-30)].

Therefore, given the teachings of Chaum, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Fujoka by employing the well known feature of determining correspondence in a blind signature scheme as disclosed above by Chaum, for which a Blind Signature process will be enhanced [pg.7, lines 25-30].

Prior Art Made of Record

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Neff et al. (US Patent No. 7,099,471)

Response to Arguments

Applicant's Remarks Claim Objection

Examiner withdraws claim objections for claims 10-18 in view of applicant's amendment.

Applicant's Remarks 101 Rejection

Examiner withdraws 101 rejection for claims 12, 14, 16, and 18 in view of applicant's amendment.

Applicant' s Remarks 102 Rejection

Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection. The Examiner contends the combined

teachings of Fujoka and Chaum provides for creating a link between signed data elements and tracing capability within a electronic voting system.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431